Assured Resource Sharing in Ad-hoc Collaboration

DE-FG02-10ER25984

DOE PI Meeting, March 1-2, 2012

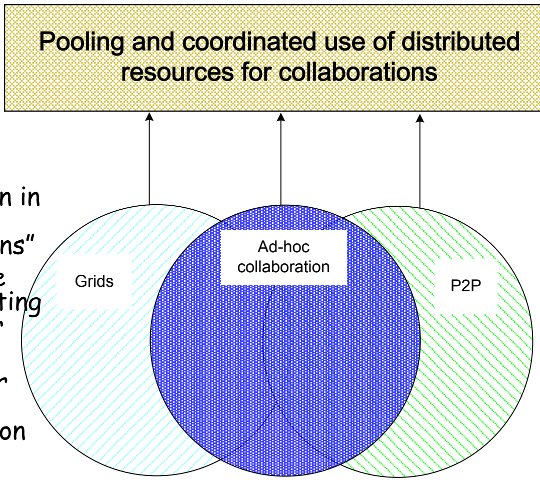
Gail-Joon Ahn

Computer Science and Engineering

ASU Ira A. Fulton school of engineering ARIZONA STATE UNIVERSITY

U.S. DEPARTMENT OF ENERGY

Technologies for ad-hoc collaboration



Pooling and coordinated use of distributed resources for collaborations

Grids

Ad-hoc collaboration

P2P

- Stable collaboration in community based "virtual organizations"
- High administrative overhead in supporting direct user-to-user communication
- Secure services for job submission and interactive execution

- Little incentive of cooperation
- Decentralized control for direct user communication and ad-hoc sharing groups.
- Non-secure data sharing and data exchanging

Characteristics of ad-hoc collaboration

- Ad-hoc collaboration is a newly emerged environment for distributed communities
  - Highly dynamic and distributed
  - Collaboration is triggered at any point and by ad-hoc events
  - Loosely established collaboration relationships among strangers
  - No pre-established infrastructure and trust base available for information sharing

Problem statement

- Information sharing in ad-hoc collaboration is always *conditional,* and needs to be *highly controlled.*
- Approaches
  - Secure sharing in Grids and Cloud
    - Effective access control framework [1]
    - Dynamic Audit Services [2]
  - Policy analysis for assurance [3] [4]
  - Risk-aware network assurance [5]

Selected results

[1] **Gail-J. Ahn**, Jing Jin* and Mohamed Shehab, "Policy-driven Role-based Access Management for Ad-hoc Collaboration," *Journal of Computer Security*, 2012 (In press).

[2] Yan Zhu, **Gail-J. Ahn**, Hongxin Hu*, Stephen S. Yau and Ho G. An, "Dynamic Audit Services for Outsourced Storages in Clouds," IEEE Transactions on Services Computing, 2012 (In press).

[3] Hongxin Hu*, **Gail-J. Ahn** and Ketan Kulkarni*,"Detecting and Resolving Firewall Policy Anomalies," *IEEE Transactions on Dependable and Secure Computing*, 2012 (In press).

[4] Ziming Zhao*, Hongxin Hu*, **Gail-J. Ahn** and Ruoyu Wu*, "Risk-Aware Response for Mitigating MANET Routing Attacks," *IEEE Transactions on Dependable and Secure Computing*, Vol. 9(2), pp. 250-260, 2012.

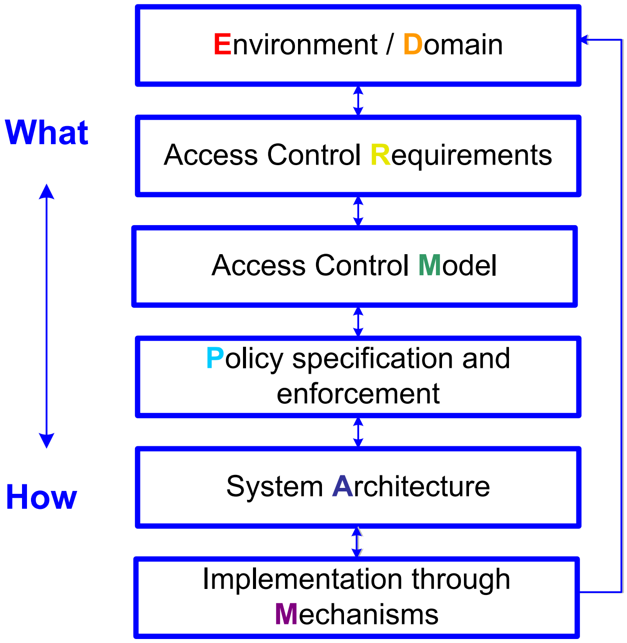
[5] Ziming Zhao*, **Gail-J. Ahn** and Hongxin Hu*, "Automatic Extraction of Secrets from Malware," *Proc. of 18th Working Conference on Reverse Engineering (WCRE),* Limerick, Ireland, October 17- 20, 2011.

* indicates students

Problem statement

- Information sharing in ad-hoc collaboration is always *conditional,* and needs to be *highly controlled.*
- Approaches
  - Secure sharing in Grids and Cloud
    - Effective access control framework [1]
    - Dynamic Audit Services [2]
  - Policy analysis for assurance [3] [4]
  - Risk-aware network assurance [5]

Systematic research approach



Environment / Domain

Access Control Requirements

Access Control Model

Policy specification and enforcement

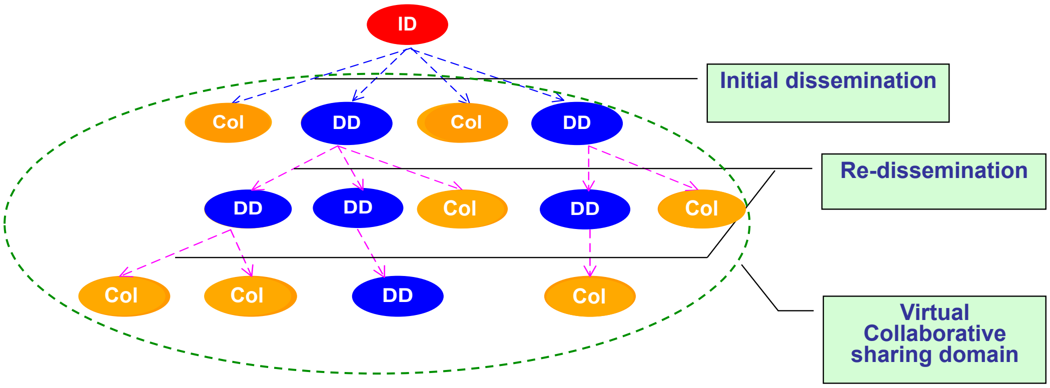
System Architecture

Implementation through Mechanisms

What

How

Access Control Requirements -- Information sharing flow



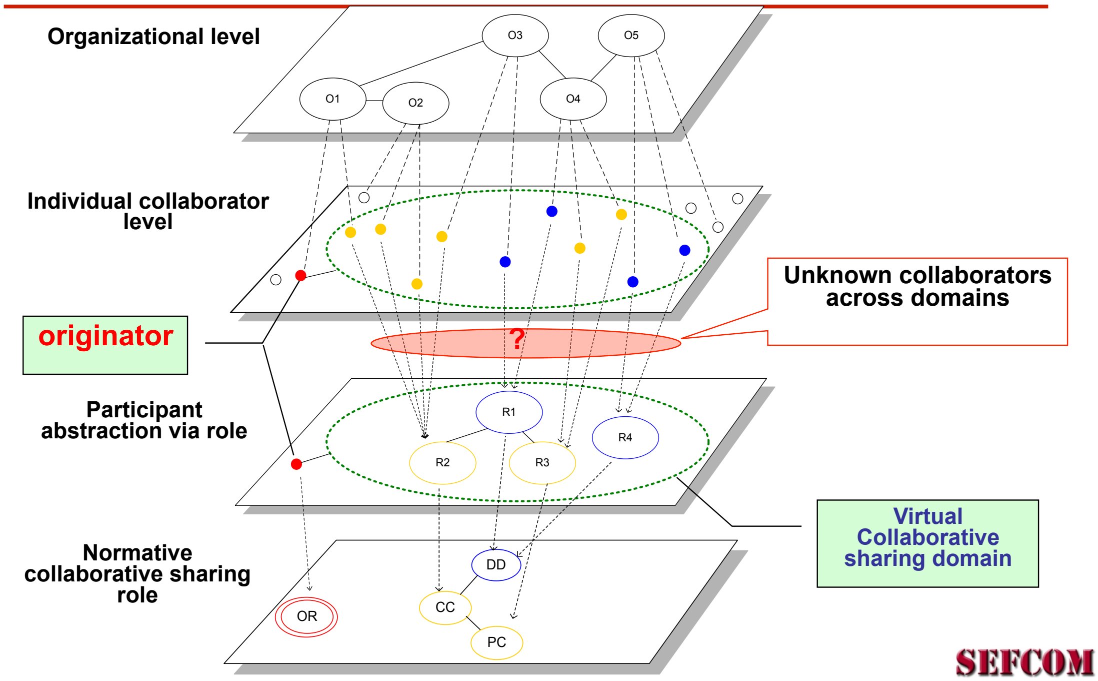
Initial dissemination

Re-dissemination

Virtual Collaborative sharing domain

- Access management requirements:
  - The originator needs an effective way to define the virtual collaborative sharing domain and authorize the unknown collaborators inside the domain
  - Access control should guarantee the sharing occurs within the originator's collaborative sharing domain, and sharing behaviors must be well regulated

Role-based approach (RAMARS)



Organizational level

Individual collaborator level

originator

Unknown collaborators across domains

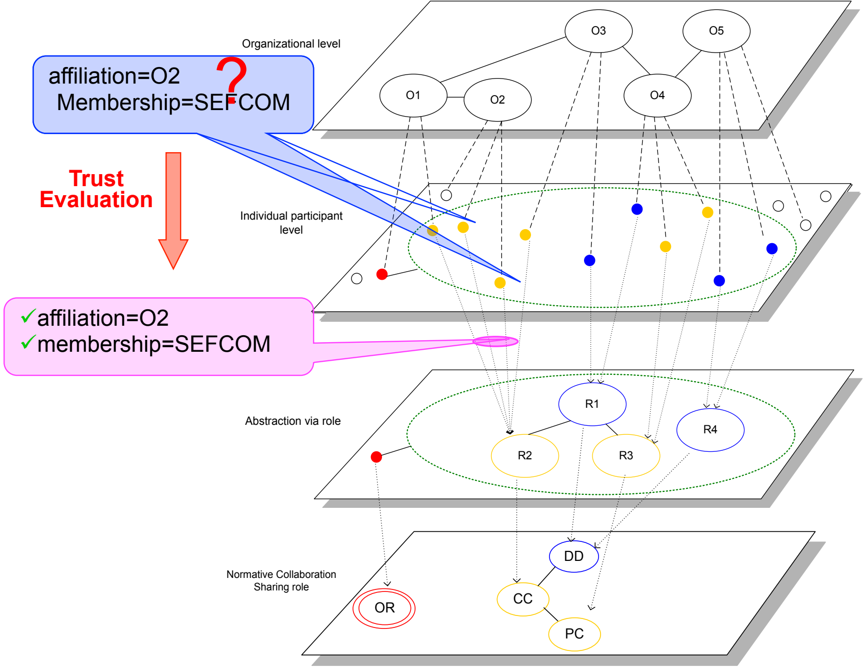
Participant abstraction via role

Virtual Collaborative sharing domain

Normative collaborative sharing role

SEFCOM

Trusted attribute-based role assignment



affiliation=O2
Membership=SEFCOM

Trust Evaluation

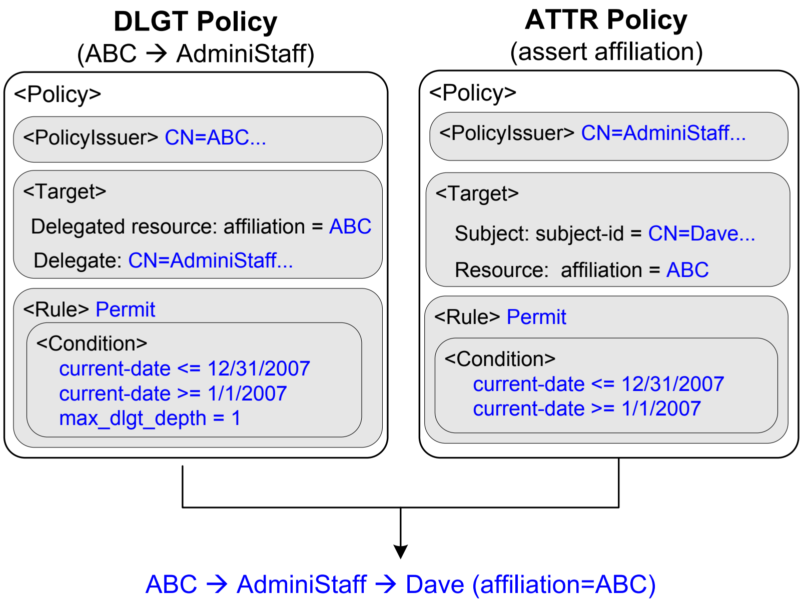
✓affiliation=O2
✓membership=SEFCOM

SEFCOM

Trust evaluation

- Observations:
  - Attributes are asserted by multiple authorities
    - e.g. "name=John" through org card, Gov card, and so on
  - Attribute assertion can be achieved through a chain of delegation.
    - e.g. ASU→ Registrar → "name=John"
- Affecting factors for trust evaluation:
  - Credential authority
  - Number of supportive credentials
  - Depth of delegation chain
- Trust level is introduced to measure the degree of trust
- Only attributes that achieve the required level of trust are promoted to the role assignment

Policy Specification



DLGT Policy
(ABC → AdminiStaff)

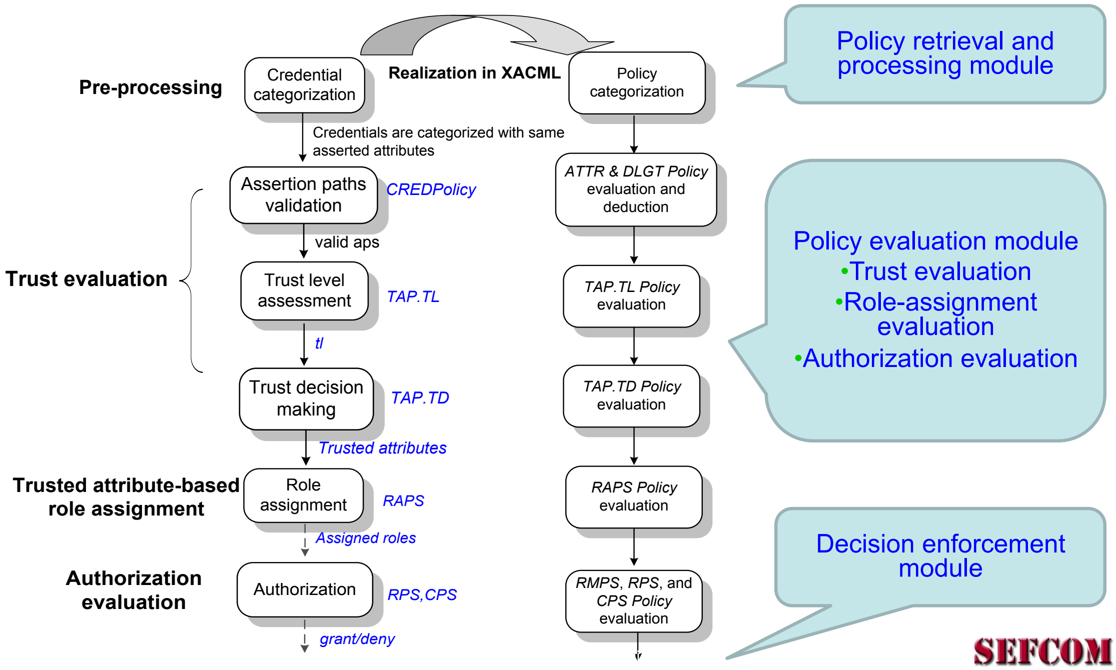
```
<Policy>
  <PolicyIssuer> CN=ABC...
  <Target>
    Delegated resource: affiliation = ABC
    Delegate: CN=AdminiStaff...
  <Rule> Permit
    <Condition>
      current-date <= 12/31/2007
      current-date >= 1/1/2007
      max_dlgt_depth = 1
```

ATTR Policy
(assert affiliation)

```
<Policy>
  <PolicyIssuer> CN=AdminiStaff...
  <Target>
    Subject: subject-id = CN=Dave...
    Resource:  affiliation = ABC
  <Rule> Permit
    <Condition>
      current-date <= 12/31/2007
      current-date >= 1/1/2007
```

ABC → AdminiStaff → Dave (affiliation=ABC)

Policy evaluation

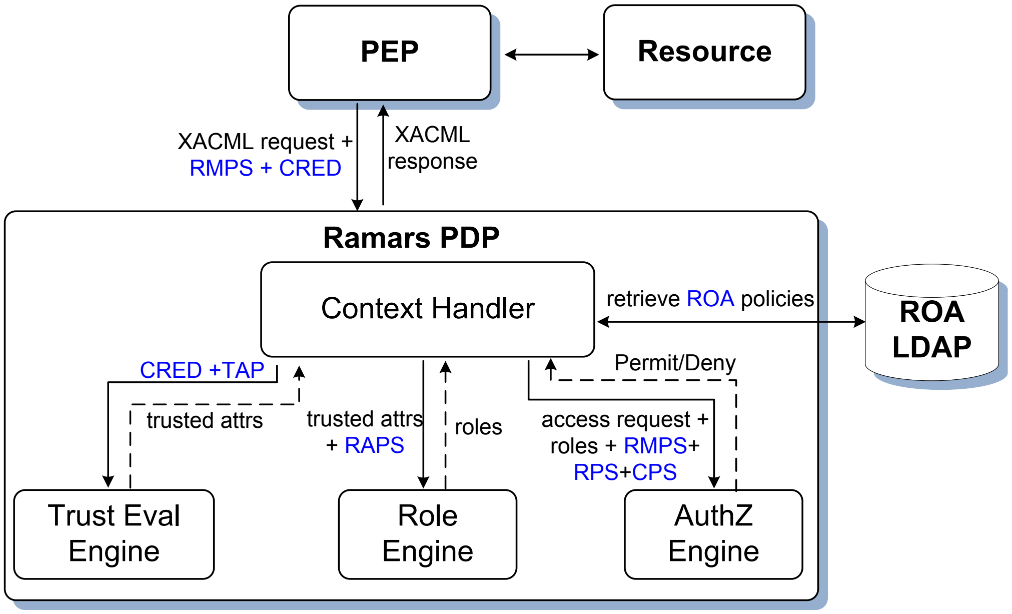


Policy retrieval and processing module

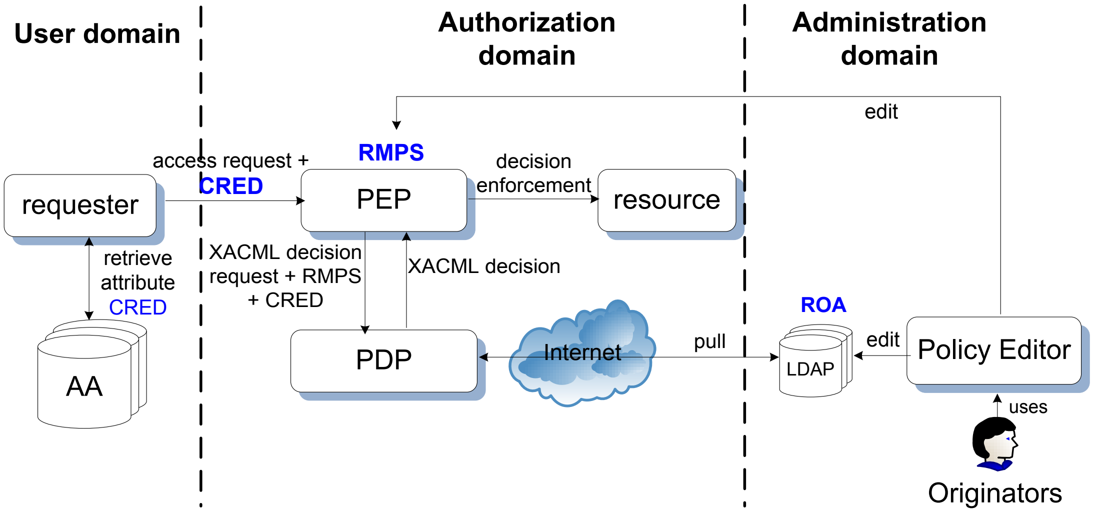
Policy evaluation module
- Trust evaluation
- Role-assignment evaluation
- Authorization evaluation

Decision enforcement module

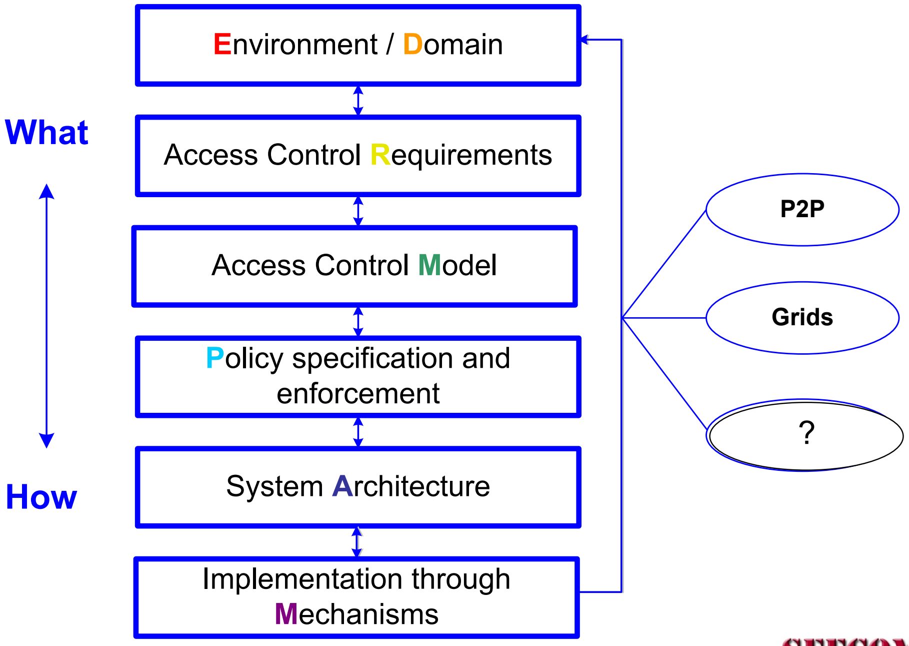
Enforcement system architecture



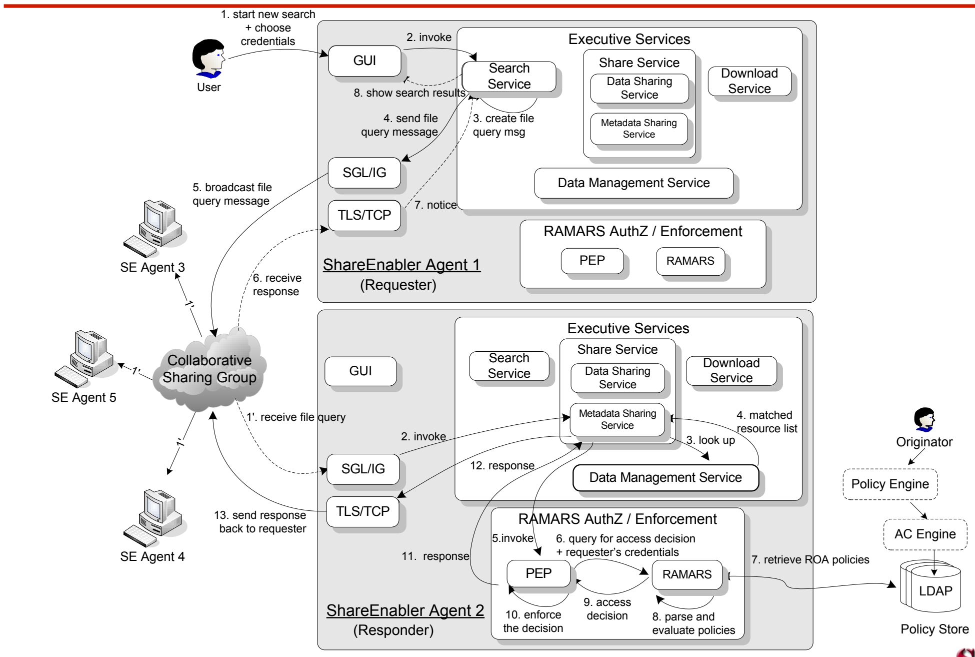
RAMARS system architecture cont’d



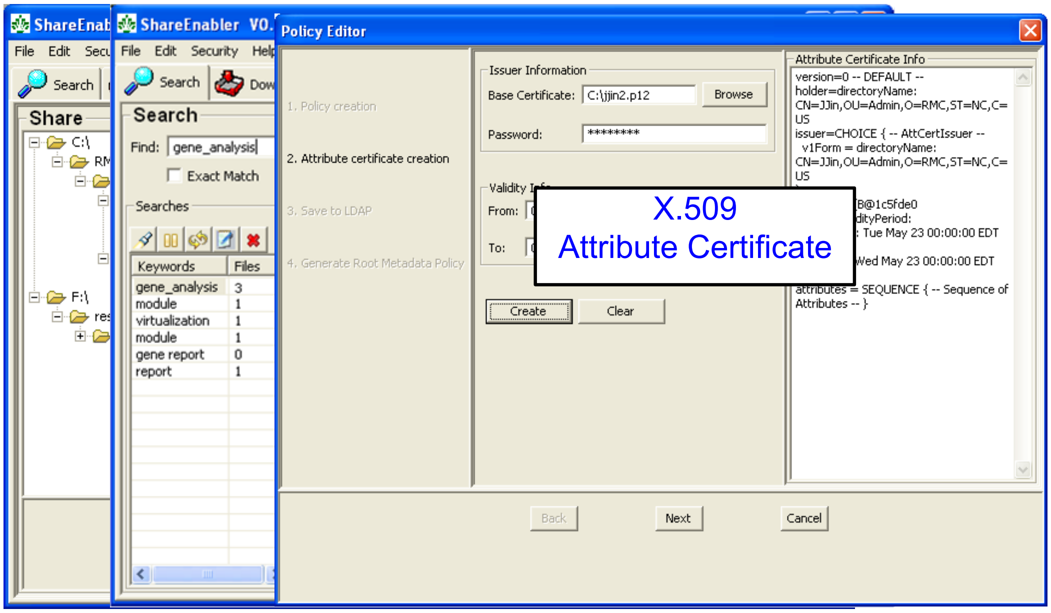
Systematic research approach


Environment / Domain
What
Access Control Requirements
Access Control Model
Policy specification and enforcement
System Architecture
How
Implementation through Mechanisms
P2P
Grids
?

RAMARS in P2P – ShareEnabler system



RAMARS in P2P -- implementation



Search

Find: gene_analysis

□ Exact Match

Searches

Keywords	Files
gene_analysis	3
module	1
virtualization	1
module	1
gene report	0
report	1

1. Policy creation

2. Attribute certificate creation

3. Save to LDAP

4. Generate Root Metadata Policy

Issuer Information

Base Certificate: C:\jjin2.p12 Browse

Password: ********

Validity Info

From:

To:

Create Clear

Attribute Certificate Info

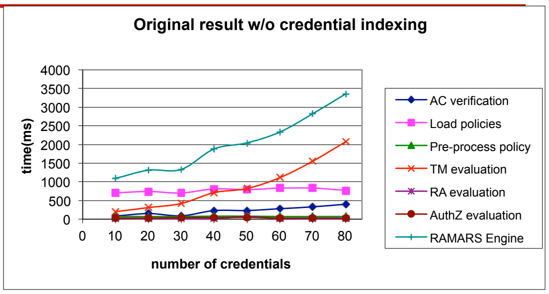
```
version=0 -- DEFAULT --
holder=directoryName:
CN=JJin,OU=Admin,O=RMC,ST=NC,C=
US
issuer=CHOICE { -- AttCertIssuer --
  v1Form = directoryName:
CN=JJin,OU=Admin,O=RMC,ST=NC,C=
US
B@1c5fde0
dityPeriod:
: Tue May 23 00:00:00 EDT
Wed May 23 00:00:00 EDT
attributes = SEQUENCE { -- Sequence of
Attributes -- }
```

Back Next Cancel

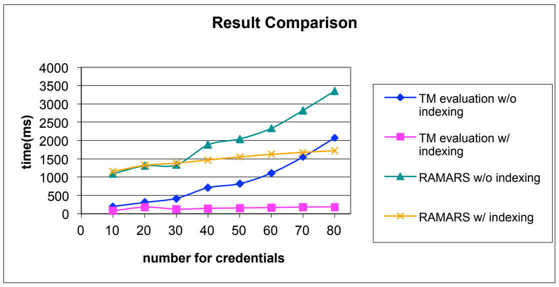
X.509
Attribute Certificate

RAMARS in P2P – Experiment 1 credential increase

- Increase in the number of credentials would affect the performance of trust evaluation

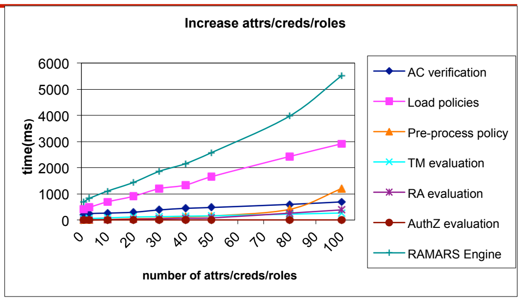


- Improvement 1 – credential indexing
  - Implement a map-based indexing mechanism to improve the trust evaluation performance

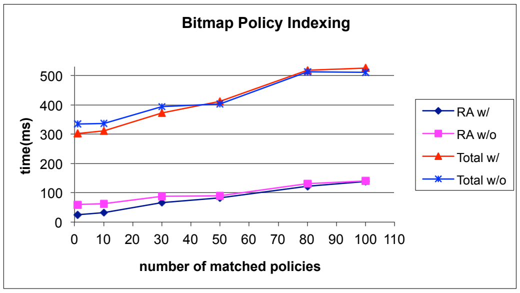


RAMARS in P2P – Experiment 2 role and attribute increase

- Increase in the number of attributes and roles would affect the role assignment and authorization evaluation



- Improvement 2 – bitmap policy indexing
  - Using bitmap and bit-wise comparison to expedite the role assignment evaluation



RAMARS in P2P – Experiment 3 overhead measurement

- Measure the overhead introduced by RAMARS authorization to scientific P2P data sharing

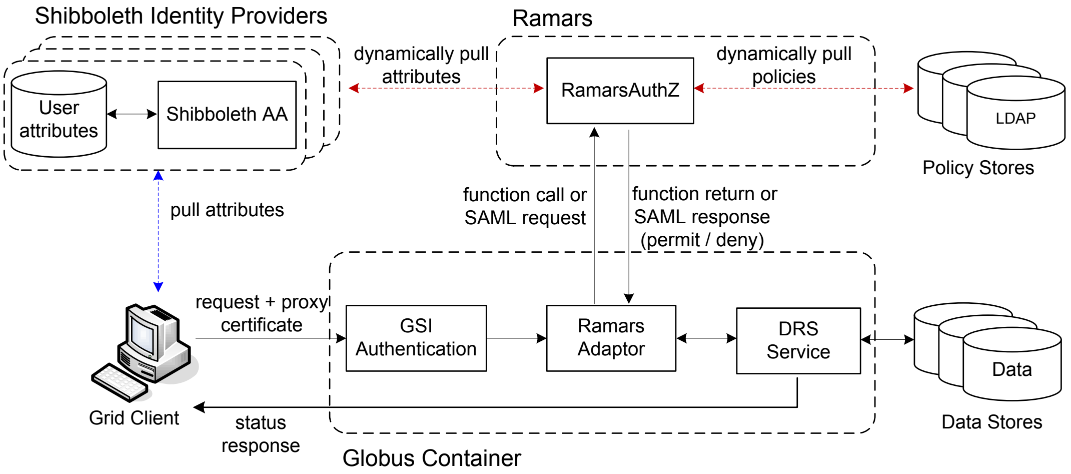
RAMARS Overhead Analysis

Test case (*attr,cred,role*)	Base	(10,10,10)	(20,20,20)	(30,30,30)
Total time (*seconds*)	487.5	488.0	489.0	490.8
Overhead (*%*)	0.00	0.10	0.30	0.68
Test case (*attr,cred,role*)	(40,40,40)	(50,50,50)	(80,80,80)	(100,100,100)
Total time (*seconds*)	492.8	495.4	499.8	508.3
Overhead (*%*)	1.07	1.61	2.53	4.27

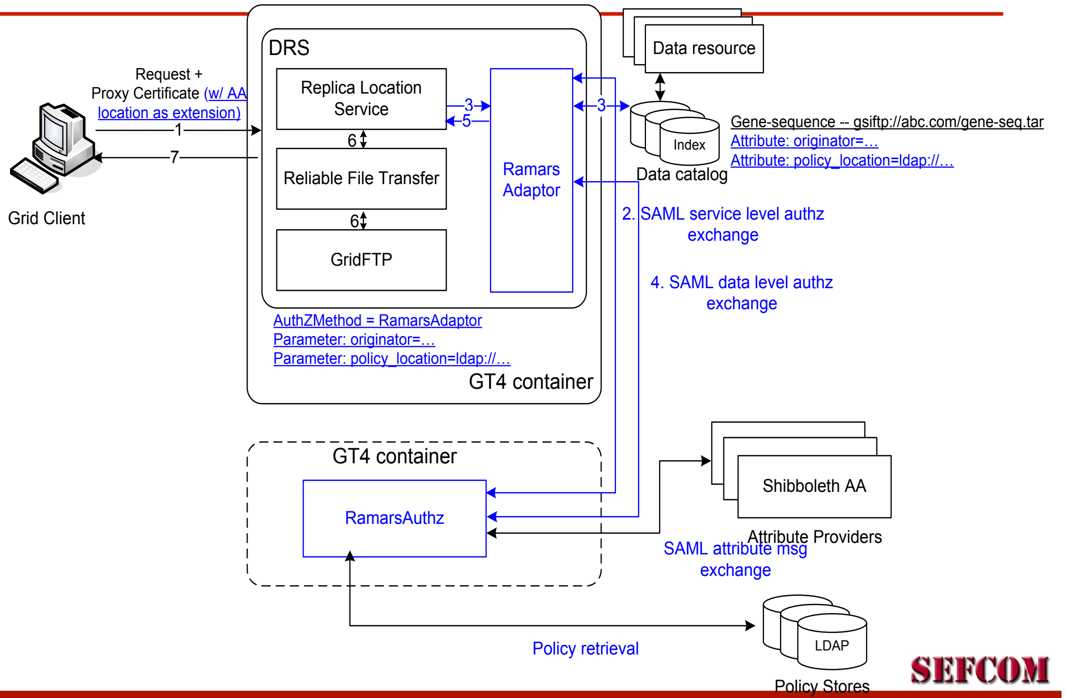
RAMARS in Grids

- Grid computing is a more structured and comprehensive collaborative sharing infrastructure
- Challenges
  - Service-oriented trend and Grid authorization service
  - Attributes from physical and virtual authorities
    - Push vs. Pull
  - Service-level control and data level control
  - Interoperability with various Grids standards and services

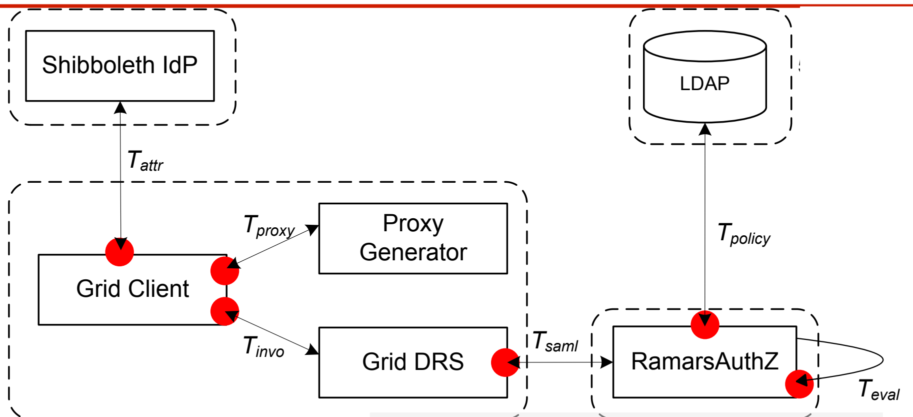
RAMARS in Grids – RamarsAuthZ service

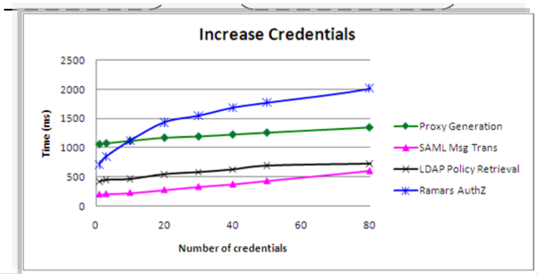

Shibboleth Identity Providers
User attributes
Shibboleth AA
dynamically pull attributes
Ramars
RamarsAuthZ
dynamically pull policies
LDAP
Policy Stores
pull attributes
function call or SAML request
function return or SAML response (permit / deny)
request + proxy certificate
GSI Authentication
Ramars Adaptor
DRS Service
Data
Data Stores
Grid Client
status response
Globus Container

RAMARS in Grids – RamarsAuthZ operations


Request +
Proxy Certificate (w/ AA location as extension)
1
7
Grid Client
DRS
Replica Location Service
Reliable File Transfer
GridFTP
6
6
3
5
3
Ramars Adaptor
AuthZMethod = RamarsAdaptor
Parameter: originator=…
Parameter: policy_location=ldap://…
GT4 container
Data resource
Index
Data catalog
Gene-sequence -- gsiftp://abc.com/gene-seq.tar
Attribute: originator=…
Attribute: policy_location=ldap://…
2. SAML service level authz exchange
4. SAML data level authz exchange
GT4 container
RamarsAuthz
Shibboleth AA
Attribute Providers
SAML attribute msg exchange
Policy retrieval
LDAP
Policy Stores

RAMARS in Grids – Testbed for performance evaluation





Problem statement (revisited)

- Information sharing in ad-hoc collaboration is always *conditional,* and needs to be *highly controlled.*
- Approaches
  - Secure sharing in Grids and Cloud
    - Effective access control framework [1]
    - Dynamic audit services [2]
    - Policy composition and schema integration
  - Policy analysis for assurance [3] [4]
  - Risk-aware network assurance [5]

Thank you!

Looking forward to collaborating with you!!

http://sefcom.asu.edu